PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04L 9/32, H04Q 7/38

A1

(11) International Publication Number: WO 00/48358

(43) International Publication Date: 17 August 2000 (17.08.00)

(21) International Application Number: PCT/EP00/01076

(22) International Filing Date: 10 February 2000 (10.02.00)

(30) Priority Data:
9903124.7 11 February 1999 (11.02.99) GB

(71) Applicant *(for all designated States except US)*: NOKIA NETWOKS OY [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: HUIMA, Antti [FI/FI]; SMT 10 F 85, FIN-02150 Espoo (FI).

(74) Agent: STYLE, Kelda, Camilla, Karen; Page White & Farrer, 54 Doughty Street, London WC1N 2LS (GB).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: AN AUTHENTICATION METHOD

(57) Abstract

An authentication method for authenticating communication between a first and a second party using a third party which is trusted by said first and second parties comprising the steps of calculating by the trusted third party the value of a first authentication output using a paramater of the first party and a second authentication output using the first authentication output and sending the second authentication output to the second party; calculating by the first party the first authentication output and sending the first authentication output to the second party; and calculating by the second party the second authentication output based on the first authentication output received from the first party and comparing the calculated second authentication output with the second authentication output received from the trusted third party whereby if the two second authentication outputs are the same, the first party is authenticated.

AN AUTHENTICATION METHOD

The present invention relates to an authentication method for use for example, but not exclusively, in wireless cellular telecommunication networks and also to a system using this method.

A typical cellular wireless network 1 is shown in Figure 1. The area covered by the network is divided into a number of cells 2. Each cell 2 is served by a base transceiver station 4 which transmits signals to and receives signals from terminals 6 located in the respective cell associated with a particular base transceiver station 4. The terminals may be mobile stations which are able to move between cells 2. As the transmission of signals between the terminal 6 and the base transceiver stations 4 is via radio waves, it is possible for unauthorised third parties to receive those signals.

Accordingly, in known wireless cellular networks, authentication is provided to identify the right mobile and ciphering is used to prevent third parties from listening in. Illustrated in Figure 2 is the procedure carried out in the GSM (Global System for Mobile communications) standard. In the first step S1, the mobile station MS makes a request to a mobile services switching centre (MSSC) via the base station for an outgoing call. A visitor location register (VLR) is informed via the mobile services switching centre of this request. The VLR takes control of the authentication procedure.

Each mobile terminal is provided with an identification number which is sometimes referred to, in a GSM standard, as the IMSI (International mobile subscriber identity) number. The MSSC forwards the mobile's IMSI to the VLR. Information on the IMSI is initially provided by the mobile station. The VLR then sends, in the second step S2, the IMSI together with the identity of the VLR to the home location register HLR of the mobile. This ensures that any incoming calls can be directed to the mobile station at communication between a first and a second party using a third party which is trusted by said first and second parties comprising the steps of calculating by the trusted third party the value of a first authentication output using a parameter of the first party and a second authentication output using the first authentication output and sending the second authentication output to the second party; calculating by the first party the first authentication output and sending the first authentication output to the second party; and calculating by the second party the second authentication output based on the first authentication output received from the first party and comparing the calculated second authentication output with the second authentication output received from the trusted third party whereby if the two second authentication outputs are the same, the first party is authenticated.

The method may comprise the steps of calculating by the first party the value of the second authentication output, sending the value of the second authentication output calculated by the trusted third party to said first party and comparing at the first party the calculated value of the second authentication output calculated by the first party and the value of the second authentication output connected by the third party whereby the second party is authenticated.

Preferably, the value of the second authentication output calculated by the trusted third party is sent to the first party by the second station.

Preferably at least one and more preferably both of the first and second authentication outputs are the outputs of a hash function. The use of a double hash function is particularly advantageous in providing a secure method of communication.

Both of the first and second hash function are preferably one way. This means that it is virtually impossible for a third party to determine the value of the at least one parameter. Preferably, calculation of the shared secret.

The trusted further party preferably has a secure connection with the second party.

Preferably the identity of at least one party is only sent to the other party in an encoded form. For example, the identity may be included within one of the first and second authentication outputs. Alternatively the identity may be sent in a separately encrypted form. Since the identity of a party is important in retaining secure communication, it is important that unauthorised third parties be not be able to obtain any identity of the first or the second party.

Preferably, the method is used in a telecommunications network which may be wired or a wireless network. One of the first and second parties may be a mobile station whilst the other may be a base station.

According to a second aspect of the present invention, there is provided an authentication method for authenticating communication between a first and a second party comprising the steps of calculating the value of a first hash function of a second hash function using at least one parameter; sending the calculated value of the first hash function of the second hash function from the first party to the second party, said second party being provided with a separately calculated value of the first hash function of the second hash function using the same at least one parameter; and comparing the value of the first hash function of the second hash function received from the first party with the separately calculated value of the first hash function of the second hash function, whereby if the two values are the same, the first party is authenticated.

For a better understanding of the present invention and as to how the same may be carried into effect, reference will now be made by way of example to the accompanying drawings in which:-

remainder when divided by the modulus n is used.

g - generator of Diffie-Hellman key exchange. g can be any suitable integer between 2 and n-1 inclusive.

x, y - random exponents used in the Diffie-Hellman key exchange. In other words, g is raised to the power of x and/or y.

R, R' - random numbers, also referred to as nonces. Typically these random numbers are changed regularly.

P, P' - security parameters - which include information as to the available ciphers, hash functions etc.

$SIG_A(\varphi)$ - signature SIG of φ by A's signature key.

$E_k(\varphi)$ - φ encrypted using key k.

$hash[X](\varphi)$ - parametrized hash function with a constant parameter X. In other words, the hash function varies in accordance with a given parameter X. The value of the parameter can of course vary.

$\varphi|X$ - concatenation (i.e. putting two items together one after the other) of φ and X.

φ,X - concatenation of φ and X.

Embodiments of the present invention use signature functions SIG having the following features. $SIG_A(\varphi)$ should only be computable by A and principals authorised by A only, assuming that φ has previously been chosen and φ has not previously been signed. In

X determines the hash function and because X only determines the functions used it does not need to be secret. Indeed, the parameters X may be publicly known and fixed for a long period of time.

The protocols which will be described hereinafter are used to perform key exchange, key reexchange and mutual authentication. In summary, the mobile station MS and the network or base transceiver station BTS perform an initial key exchange protocol in order to obtain a shared secret S as a result of a Diffie-Hellman key exchange. This shared secret S is g^{xy}mod n. The parties also exchange a pair of random numbers R, R'. The concatenation of the shared secret S and the two nonces provide the key material. Different keys are derived from key material using different parametrized hash functions. Rekeying is performed by exchanging a new pair of random numbers.

Keys for encrypting further communications can also be created using the following formula: $k=\text{hash}[T](g^{xy}\text{mod } n|R|R')$ where T is a unique parameter. T can be public or fixed and can be used once or more than once.

During the initial key exchange protocol, security parameters P are exchanged. These security parameters are used to inform the other party about the available ciphers, hash functions etc.

Diffie-Hellman key exchange is a way to establish a shared secret between two parties. When using modular arithmetic, it is very hard to compute the value of x when only g^x is known. Normally, computing x from g^x means computing the logarithm of g^x and this is easy. However, in modular arithmetic the situation changes dramatically; it is not known how to compute x from g^x.

In Diffie Hellman key exchange therefore two parties establish a shared secret in the following way. The first party sends "g^x". The second party sends "g^y". Here x is known only by the first party and y is known only by the second party. However the values

The signature SIG_B provided in the second message by the base transceiver station is as follows:

$$SIG_B(hash[SIG1](n|g|g^x|g^y|g^{xy}|P|P'|R|R'|B))$$

B is the identity of the base transceiver station.

A temporary key k is computed from the shared secret and the random numbers. The random numbers are included in the temporary key so that rekeying can occur using the same shared secret. Rekeying occurs when a new temporary key is generated. As will be described in more detail hereinafter, rekeying can be achieved by providing new random numbers R and R'. The temporary key k is equal to $hash[TKEY](g^{xy} mod\ n|R|R')$.

The mobile station carries out a verify function in respect of the signature SIG_B. The verify function and the signature function are related so that given the value of the signature function, the verify function provides an accept or reject value. Accept means that the signature is accepted and reject means that the signature is invalid. In other words the mobile station is arranged to verify the signature which it receives.

In step A3, the message which is sent from the mobile station MS to the base transceiver station is encrypted using the temporary key. In the encrypted message, the identity of the mobile user U is included. Thus, the identity of the user U is only sent in an encrypted form. The encrypted identity is represented by $E_k(U)$. Along with the encrypted identity, the mobile station also sends a signature SIG_U, similar to that sent from the base transceiver station to the mobile station in step A2. However, that signature is encrypted. The encrypted signature is represented by the following:

$$E_k(SIG_U(hash[SIG2](n|g|g^x|g^y|g^{xy}|P|P'|R|R'|B|U))).$$

As can be seen, the identity of the mobile user is included in the signature. Encryption of the signature is not essential although the mobile's identity is encrypted and it may be more convenient also to encrypt the signature. It should be the base transceiver station BTS sends the following authenticating hash function to the trusted third party TTP:

$$hash[AUTH](n|g|g^x|g^y|g^{xy}|P|P'|R|R'|B|U)$$

The identity of the mobile user U is already known by the trusted third party. This may be achieved in any suitable way.

In embodiments of the present invention, it is preferred to send the hash of g^{xy} rather than the encryption key k. As the encryption key k is probably shorter than g^{xy}, it is thus easier to attack. First shared secret data g^{xy} mod n is assumed to be shared by the base station and the mobile but by no-one else. There is a second, long term, shared secret between the base station and the mobile phone which is distributed offline. This long term secret may be in the SIM card of the mobile phone or the like. The first secret g^{xy} modn used to get a session key whilst the second secret is used so that the mobile phone is able to authenticate the base station.

In the fifth step B5, the trusted third party computes a hash of the secret from the shared secret data concatenated with hash [AUTH] which the base transceiver station sent thereto. A hash of the hash value calculated by the trusted third party is then calculated, again by the trusted third party. The trusted third party then sends this finally computed hash value to the base transceiver station which records this value. The value sent by the trusted third party to the base transceiver station is as follows:

$$hash[RESP](hash[SEC](S|hash[AUTH](n|g|g^x|g^y|g^{xy}|P|P'|R|R'|B|U)))$$

The same value is then forwarded from the base transceiver station to the mobile station in the sixth step B6. The mobile station is able to compute the value of hash [SEC] directly. The mobile station then calculates hash [RESP] from hash [SEC] and thus compares the value of hash [RESP] (hash [SEC]) which it calculated with the value received from the trusted third party via the base transceiver station. If the two values of the same information which is sent in the key exchange using signatures (Figure 3) and also signs the information. With this key exchange, the base station cannot be as sure as to the identity of the mobile station with which it is communicating. However, the signature by the base transceiver station ensures good key exchange. In other words, the unidentified mobile station can detect if there are any man in the middle of attacks and drop the connection if needed. The base station is not able to detect man in the middle attacks but it does not need to. In particular, the base station will not transmit security critical information to an unidentified party anyway. This can be used for access to public networks such as the internet where the identity of the mobile is not required.

Reference will now be made to Figure 6 which shows a simple rekeying procedure without requiring new authentication. The purpose of this protocol is to distribute new random numbers in order to perform rekeying.

Re-keying means that a new temporary key k for encryption purposes can be generated. To avoid the unauthorised deciphering of messages between the mobile station and the base station, rekeying should occur frequently.

In the first step D1, the mobile station sends to the base transceiver station the new random number R_{new}. In the second step D2, the base transceiver station transmits a second new random number R'_{new} to the mobile station. With this particular protocol, it is not necessary that the random numbers be kept secret. However, the integrity of the random numbers should be protected. In other words, the random numbers should not be modified during their transmission between the mobile station and the base transceiver station. This is for issues of quality and not security. It is of course possible that the order of the two steps D1 and D2 can be reversed.

A new temporary key k can be derived from the equation

In the first step F1, the mobile station sends the new random number R_{new} to the base transceiver station. In the second step, F2, the base transceiver station sends the second new random number R'_{new} to the mobile station and signs a signature hash function as follows:

$$SIG_B(hash[SIG1](n|g|g^x|g^y|g^{xy}|P|P'|R_{new}|R'_{new}|B))$$

The mobile station is able to calculate a new encryption key using these new random numbers as outlined hereinbefore. The mobile station is also able to authenticate the base station using a verification function.

The new encryption key k is therefore hash[TKEY](g^{xy}mod n| Rnew| R'new). In the third step F3, the mobile station sends to the base transceiver station an encrypted signature of a hash function hash[SIG] having the following form: $E_k(SIG_U(hash[SIG2](n|g|g^x|g^y|g^{xy}|P|P'|R_{new}|R'_{new}|B|U)))$. The signature sent by the mobile station is encrypted. This is not essential but may be more convenient with other information needs to be encrypted. The encryption uses the new encryption key k. The base station is able to authenticate the mobile station by verifying the signature. If the verification function is accepted, the mobile station is authenticated.

Reference will now be made to Figure 9 which shows rekeying using third party authentication. In the first step G1, the mobile station sends to the base station the identity of the new random number R_{new}. In the second step G2, the base transceiver station sends to a trusted third party an authentication hash function $hash[AUTH](n|g|g^x|g^y|g^{xy}|P|P'|R_{new}|R'_{new}|B|U)$ along with the mobile identity U. The authentication hash function includes a second new random number R'new. As the connection between the base station and the trusted third party is secure, there is no need to encrypt the identity of the mobile station U. The trusted third party computes in the third step G3 a hash [RESP] of a hash of the shared secret S which includes the authentication hash function and the shared secret and sends this value to the base

11. $E_K(SIG_u(hash[SIG2](n|g|g^x|g^y|g^{xy}|P|P'|R|R'|B|U))$
12. $E_K(U)$
13. $hash[AUTH](n|g|g^{xy} mod\ n|R|R'|B|U)$, U
14. $hash[RESP](hash[SEC]S|hash[AUTH](n|g|g^{xy} mod\ n|R|R'|B|U))$
15. $hash[SEC](S|hash[AUTH](n|g|g^{xy} mod\ n|R|R'|B|U))$

As it can be seen, some of these messages share a common structure namely messages 2 and 3, messages 4 and 5, and messages 6 and 7. This leaves a total of 12 different types of message. This protocol family is thus advantageous in that it allows a relatively large number of different protocols to be implemented using only a small number of different messages.

Thus, the various different methods outlined hereinbefore can define a family of methods made up of a limited number of messages. It is thus possible, in embodiments of the present invention, to select one of those methods. Various different criteria can be used in deciding which of the methods to use. For example, the different methods can be selected at random. A re-keying method may always be selected only if a key exchange method has been previously selected. The method may be selected depending on the processing capability of the first and/or second party (or the trusted third party when provided). The method can be selected in dependence on the amount of time since the last method was used. Alternatively, the method can be selected based on the function provided by the particular method eg, whether or not a trusted third party is used and whether or not authentication is required and if so what type of authentication.

In the arrangement described hereinbefore, the mobile station is described as communicating with the base transceiver station. It should be appreciated that the communication can in fact take place with any suitable element of the network although this communication will be via the base transceiver station. In other words, some of the calculations described as taking place in the base transceiver station in the preferred embodiments may take place in other parts of the network but will be transferred to the base transceiver station where appropriate. The mobile

Embodiments of the present invention may also be used in other situations which require authentication such as other types of wireless communication or communications which use fixed wire connections. Embodiments of the present invention are not just applicable to communication networks but are also applicable to point to point connections be they wired or wireless connections.

5. A method as claimed in claim 4, wherein both of said first and second authentication outputs are the outputs of a hash function and both of said hash functions are one way.

6. A method as claimed in claim 4 or 5, wherein at least one of said hash functions has a value of at least 160 bits in length.

7. A method as claimed in any of claims 4, 5 or 6, wherein one of the hash functions includes a secret which is shared by said first and second parties.

8. A method as claimed in claim 7, wherein said secret comprises a Diffie-Hellman function.

9. A method as claimed in claims 7 or 8, wherein the shared secret is used by at least one party to encrypt communications between the first and second parties.

10. A method as claimed in any one of claims 7, 8 or 9, wherein the shared secret is g^{xy}mod n where g is a Diffie-Hellman function, x and y are random numbers and n is the modulus of the Diffie-Hellman function.

11. A method as claimed in any preceding claim, wherein at least one random number is used to encrypt communications between the first and second parties.

12. A method as claimed in claim 11, wherein rekeying of a encryption function occurs when the at least one random number is changed.

13. A method as claimed in any preceding claim, wherein the value of at least one parameter is sent from the first station to the second station.

14. A method as claimed in any preceding claim, wherein the value of at least one parameter is sent from the second station

received from the trusted third party, whereby if the two second authentication outputs are the same, the first party is authenticated.

23. A first station as claimed in claim 22, wherein said first station is a mobile station.

24. A first station as claimed in claim 22, wherein said first station is a base transceiver station.

25. A first station as claimed in claim 22, 23 or 24, wherein said first station receives the second authentication output from the trusted third party via the second station.

26. A wireless telecommunications system comprising a first station as claimed in any of claims 22 to 25 and a second station, wherein said second station is arranged to calculate the first authentication output and to transmit the first authentication output to the first party.

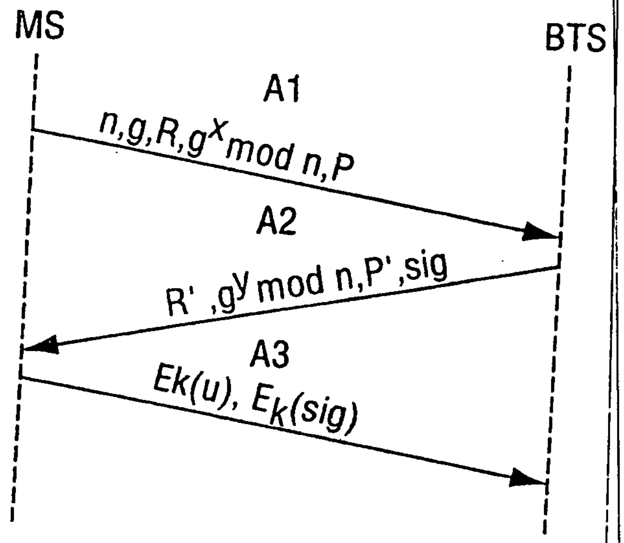
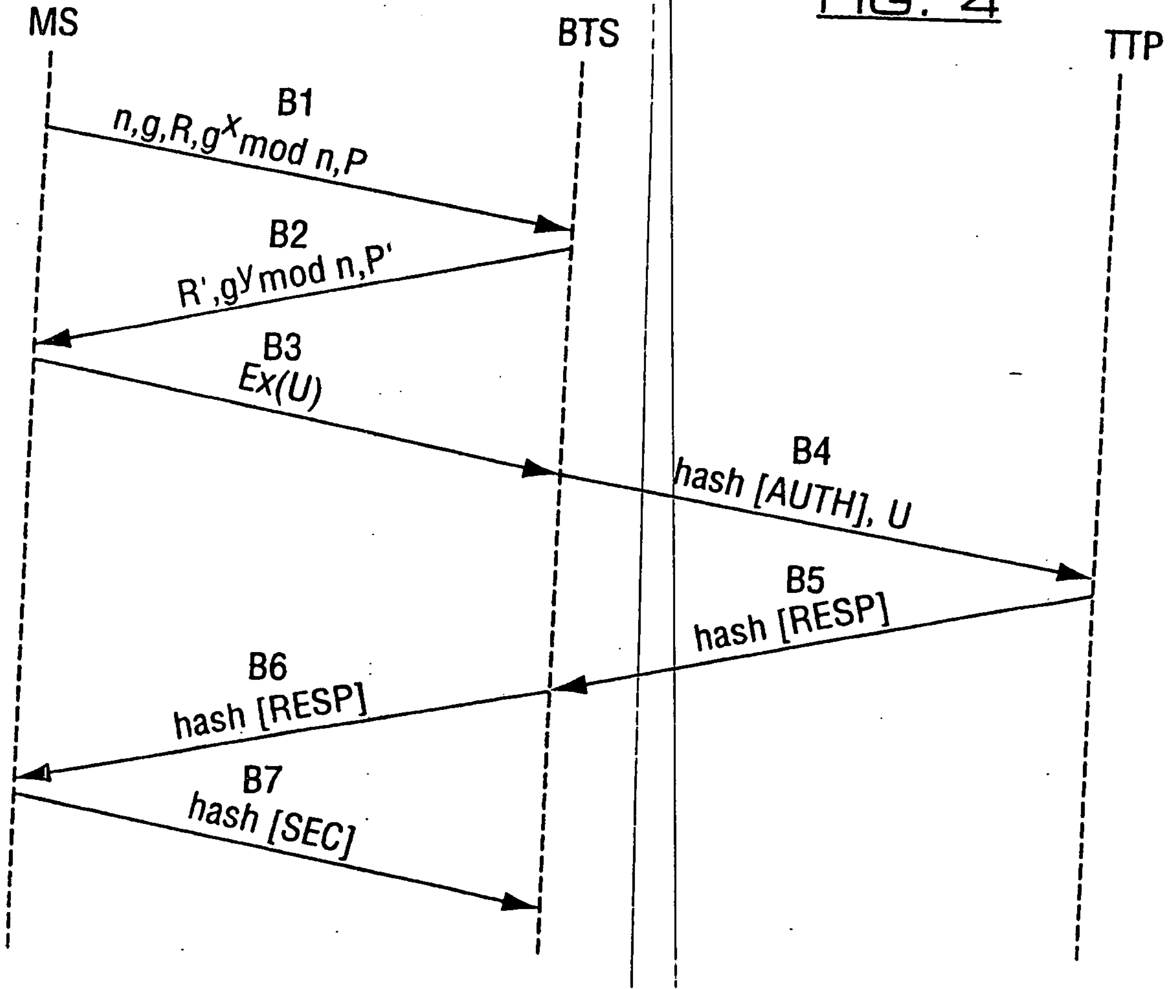

MS
BTS
A1
$n,g,R,g^x \bmod n,P$
A2
$R',g^y \bmod n,P',sig$
A3
$Ek(u), E_k(sig)$

FIG. 3

FIG. 4


MS
BTS
TTP
B1
$n,g,R,g^x \bmod n,P$
B2
$R',g^y \bmod n,P'$
B3
$Ex(U)$
B4
hash [AUTH], U
B5
hash [RESP]
B6
hash [RESP]
B7
hash [SEC]

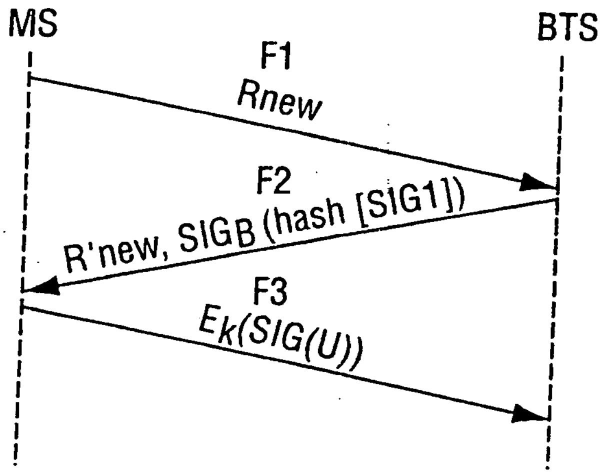

MS
BTS
F1
Rnew
F2
R'new, SIGB (hash [SIG1])
F3
Ek(SIG(U))

FIG. 8

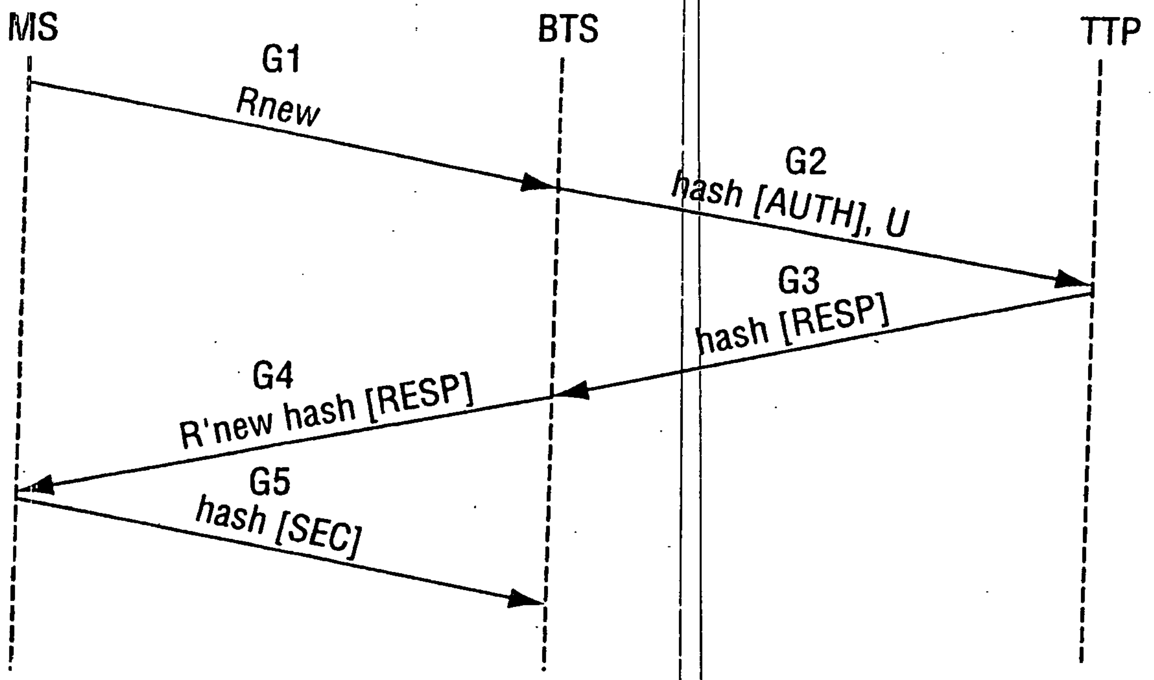

MS
BTS
TTP
G1
Rnew
G2
hash [AUTH], U
G3
hash [RESP]
G4
R'new hash [RESP]
G5
hash [SEC]

FIG. 9

INTERNATIONAL SEARCH REPORT

Int .tional Application No
PCT/EP 00/01076

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 03285 A (MOHRS WALTER ;DEUTSCHE TELEKOM MOBIL (DE); MARINGER GUENTER (DE);) 21 January 1999 (1999-01-21) page 4, last paragraph -page 5, line 8 page 6, line 1 -page 7, line 7; figures 2,3 ---	1,20-22
A	EP 0 708 547 A (AT & T CORP) 24 April 1996 (1996-04-24) column 4, line 44 - line 55 column 7, line 48 - line 22 ---	1,22
A	US 5 491 750 A (BELLARE MIHIR M ET AL) 13 February 1996 (1996-02-13) column 10, line 18 -column 12, line 4 --- -/--	1,22

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 24 May 2000	Date of mailing of the international search report 31/05/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Holper, G

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte ional Application No
PCT/EP 00/01076

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9903285 A	21-01-1999	DE 19730301 C	03-09-1998
		AU 9252098 A	08-02-1999
		EP 0995288 A	26-04-2000
EP 0708547 A	24-04-1996	US 5608778 A	04-03-1997
		CA 2156206 A	23-03-1996
		JP 8096043 A	12-04-1996
US 5491750 A	13-02-1996	NONE	
US 5666415 A	09-09-1997	NONE	